UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

CASHMAN DREDGING AND MARINE CONTRACTING CO., LLC, Plaintiff, v. FRANK BELESIMO and CALLAN MARINE, LTD, Defendants.	Civil Action No. 1:21-cv-11398-DJC Leave to file under seal granted on 08/31/21

AFFIDAVIT OF DAVID SUN

I, David Sun, hereby depose and state:

1. I am a Principal at Clifton Larson Allen, LLC ("CLA") which has been retained by Plaintiff's counsel in connection with the above-captioned matter.

2. Except as otherwise noted, I have personal knowledge of all facts and analysis set forth in this declaration. My investigation, analyses, and opinions set forth below are based upon information supplied to me by Counsel and my review of information relevant to the matter, as well as my extensive professional experience and knowledge of cybersecurity and forensic investigations. I am not a lawyer and the opinions offered in this declaration are not intended to be and should not be construed as legal opinions.

Background and Qualifications

3. I am currently the Principal in charge of the cyber forensics and incident response practice at CLA. I came to this role through CLA's acquisition of my prior company SunBlock Systems, a consulting firm that specialized in cyber security, computer forensics and technology consulting where I was the Founder and Chief Executive Officer starting in 2002 and personally

conducted numerous computer forensic examinations and investigated cyber-related intrusions and breaches.

4. In addition, I was also the co-founder and Chief Technology Officer (CTO) of S34A, Inc., a company that performed advanced research in computer forensics for the Department of Homeland Security and other government agencies. As CTO, I was responsible for the company's overall research efforts as we developed advanced computer forensics techniques and equipment for various United States government law enforcement agencies.

5. I am a Certified Information Systems Security Professional (CISSP) (arguably the most respected certification available for information systems security professionals), a Certified Computer Examiner (CCE), and an EnCase Certified Examiner (EnCE). I graduated from Virginia Polytechnic Institute and State University (aka Virginia Tech) with a Bachelor of Science and a Master of Science Degree in Electrical Engineering, and I have been an Adjunct Professor at George Mason University and a faculty member for the Virginia and Massachusetts State Bars' continuing education programs teaching courses on computer forensics and electronic evidence. I am regularly invited to speak at technical conferences and at government agencies on advancements in the field of computer forensics. I have been awarded multiple patents for inventions in the field of computer forensics, and I have authored numerous technical publications covering topics of interest in the fields of computer forensics, electromagnetics, and telecommunications.

6. I have testified as an expert witness or provided expert support in numerous litigation matters, including but not limited to matters involving digital data, computer forensics and the various technologies and techniques used to obfuscate computer activity. I have also served as an expert or managed a team of experts involved in numerous complex matters

involving data breaches, IT security, computer forensics and e-Discovery. Examples include the following:

a. Managed hundreds of computer investigations and e-Discovery matters involving various legal issues ranging from United States Security and Exchange Commission regulatory compliance and United States Environmental Protection Agency criminal investigations to investigations related to homicide, black-market drug manufacturing, intellectual property theft, identity theft, corporate malfeasance, system hacking and wrongful termination.
b. Investigated computers used by the sitting Mayor for the City of New Orleans for evidence that he destroyed public records.
c. Served as a computer forensics and e-Discovery expert for various multi-national corporations involved in class action antitrust litigation.
d. Performed information security assessments for various high-profile events such as the Games of the 2004 Olympiad in Athens, Greece; the United Nations 2002 Summit on Economic Development in Johannesburg, South Africa; and the United States Federal Reserve Bank in Dallas, TX.

Collection of Data and Monitoring User Activity

7. In June of 2021 Cashman Dredging and Marine Contracting Co., LLC ("CDMC") engaged CLA and my team through counsel to help identify and protect the CDMC intellectual property maintained by their Executive Vice President Frank Belesimo. Moreover, CDMC wanted to gain a better understanding of Belesimo's daily work activities on the CDMC computing devices.

8. As part of performing this assignment, I directed one of my staff to visit the CDMC office to surreptitiously make forensic copies of CDMC devices used by Belesimo. Using various industry standard forensic tools that are widely accepted for forensic examinations

in civil and criminal matters, we made copies of Belesimo's primary laptop and two (2) portable USB hard drives (USB1 and USB2). It is my understanding that many of the files stored on the laptop and portable USB drives are unavailable anywhere else or to others at CDMC because Belesimo did not keep a copy of his work files on the company network choosing to only store them on those devices.

9. In addition to copying the devices, I also had my staff install monitoring software on the primary laptop. This monitoring software is a surveillance tool designed to track, capture, record and log activity by a user or employee when using web browsers, instant messaging, e-mails, applications, documents and programs. Specifically, this software records the keys typed on the computer, documents reviewed or downloaded and captures a copy of computer display (i.e. screen shots) at regularly timed intervals for subsequent review.

10. On July 14, 2021, I was informed that Belesimo tendered his resignation. Upon learning this, I reviewed the monitoring software for his activities immediately preceding his resignation and uncovered various actions of concern.

Transfer of Control for CDMC Intellectual Property

11. My review revealed that on the morning of July 14, 2021, Belesimo logged into a Dropbox[1] account he created for work purposes, routinely stored work materials, and had registered to his corporate e-mail. The monitoring software captured Belesimo changing the registration from his CDMC corporate email account to his personal AT&T email account. This change effectively locked CDMC out of the account and transferred control of the account as well as all the data stored in it, to Belesimo exclusively. Figure 1 in Exhibit A shows the account

[1] Dropbox is a file hosting service, often referred to as a "cloud storage" service that allows the storage of electronic files without the need for physical devices or media. It allows a person to copy files to the service and access them later, even if they are using a different device.

registered to a CDMC email address as Belesimo changes the registration to this AT&T account and Figure 2 in Exhibit A shows the account after transfer to Belesimo's AT&T account.

12. My forensic analysis shows that Belesimo routinely stored 19,740 files and folders in the Dropbox account, the vast majority of them related to CDMC business. Exhibit B provides a list of those files and folders. Additionally, the monitoring software recorded Belesimo on July 14, 2021, the day of his departure, uploading 13,234 additional files to the Drobox account after he transferred control of the account to his personal email. Figure 3 of Exhibit A is an image where Belesimo had selected a large set of files on the right side for upload to Dropbox. In fact, in the bottom of the image, I noted a Dropbox upload progress indicator noting 11,527 files and 5 hours left to complete. Exhibit C is a listing of the files and folders I believe are shown in the screenshot being uploaded by Belesimo. In total, between Exhibits B and C I have identified 32,974 files and folders in the Dropbox account that remain under Belesimo's control after his departure from CDMC. I also believe that additional time and forensic analysis may allow me to identify additional files.

13. On top of uploading tens of thousands of CDMC documents to Dropbox and transferring control of the account to his personal email on his last day, my review of his laptop showed that he maintained an Apple iCloud account where he stored 857 files and folders, a significant number of which are CDMC documents. iCloud is a cloud storage service similar to Dropbox and documents kept in iCloud can be access later from a different device. Exhibit D provides a list of files and folders stored in Belesimo's iCloud account.

Deletion of CDMC Intellectual Property and Purge of Computer Activity

14. My review of the devices used by Belesimo showed that he deleted a significant amount of CDMC documents from those devices and purged information about his computer activity. Specifically, I found that Belesimo deleted 53,856 files and folders from his portable

USB hard drives (USB1 and USB2) throughout various times of the day on July 14, 2021. Figures 4 and 5 in Exhibit A show Belesimo's deleting files from USB1 and USB2 respectively and a listing of these files and folders is provided as Exhibit E.

15. I also determined that he uninstalled the Dropbox application at 9:30 AM on July 14, 2021 and subsequently deleted all 19,740 Dropbox files and folders stored locally on his computer. Doing this would not have removed the files from the Dropbox account but would have hidden the fact that he used Dropbox and the details about which files were stored there. Similarly, Belesimo also deleted the 857 iCloud files and folders stored locally on his computer, obscuring his use of the service and files stored there.

16. In total, I was able to identify 30,133 files and folders that were deleted from Belesimo's laptop between June 9, 2021 and his departure on July 14, 2021. Exhibit F is a listing of the 9,535 files and folders not already provided in Exhibits B and D. Figure 1 below provides a visual example of the numerous, yet targeted files that were deleted from one folder on Belesimo's. The figure shows the contents of Belesimo's Desktop folder on June 9, 2021 highlighting the files and folders no longer present on July 14, 2021. The red highlights indicate CDMC files and folders that were deleted.

Figure 1. Belesimo's Desktop Folder Deletions

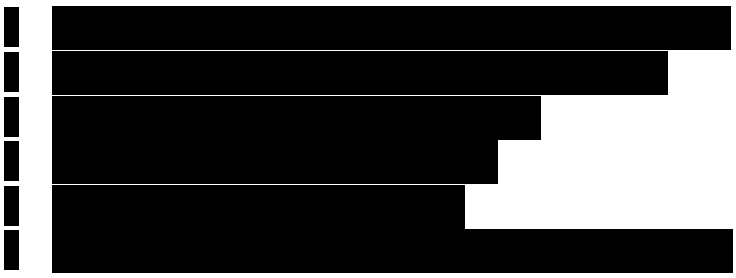
17. Along with deleting files, my review of the monitoring software captured Belesimo purging additional evidence of his computer activities. Figure 6 in Exhibit A shows Belesimo deleting his Internet browsing history and other traces of his activity. Figure 7 in Exhibit A shows Belesimo deleting System Restore and Shadow Copies of the laptop. System Restore and Shadow Copies are features in the Microsoft Windows operating system which help preserve previous states of the computer and files allowing a user to revert to a previous state in the event data is lost, deleted or corrupted. In short, deleting the System Restore and Show Copies would have made it very difficult to discover the changes and deletions Belesimo made on this computer prior to his departure and recovering the deleted information without a forensic

examination.

Unaccounted USB Devices with CDMC Intellectual Property

18. I also discovered that on July 14, 2021, Belesimo connected a USB drive labeled "SMI USB DISK USB Device" with a device identifier of "6&1f5c3a82" to his CDMC computer and transferred numerous computer files and folders, including CDMC's confidential information. Although there is no record of the entirety of what Belesimo transferred to the USB drive, except the files on the USB drive itself that Belesimo retained when he left CDMC, there is a record on his CDMC laptop of some of the files and folders opened from that USB drive while attached to the CDMC laptop. I have provided a list of the files and folders opened from the USB drive while attached to the CDMC laptop as Exhibit G. Many of the files listed contain confidential and proprietary dredge pumping and hydraulic flow data.

19. [redacted]



20. A list of the data storage devices and their identifiers is appended hereto as Exhibit H and a list of some of the files and folders on those devices and other removable media used by Belesimo is appended as Exhibit I. I have been informed by CDMC that Belesimo did not disclose nor did he provide these external data storage devices or media to CDMC when he left CDMC.

21. The full extent of Belesimo's potential misuse of CDMC devices and intellectual property is still under review. Nonetheless, based on the information I have uncovered so far, I believe that Belesimo continues to maintain control of a significant amount of CDMC intellectual property which can severely impact CDMC's business operations.

Signed under the pains and penalties of perjury the 30th of August 2021.

David Sun